APPLICATION
for
UNITED STATES LETTERS PATENT

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

Be it known that,

Inventors: Steve D. Singleton, Atlanta, GA
Brian Wong Shui, Atlanta, GA
Gary Carroll, Louisville, CO
Don Pauley, Estes Park, CO
Susan Chin, Atlanta, GA

have invented a new and useful ASSET MANAGEMENT SYSTEM of which the following is a specification.

HOLLAND & KNIGHT, LLP
Suite 2300
400 North Ashley Drive
Tampa, Florida 33602
Telephone: 813/227-8500

ATTORNEY DOCKET NUMBER: 069253.00001

ASSET MANAGEMENT SYSTEM

RELATED APPLICATION DATA

This application claims benefit of provisional patent application serial number 60/269,808 entitled "ASSET MANAGEMENT SYSTEM" filed on February 20, 2001, the contents of which are incorporated herein by reference. This application also claims benefit of provisional patent application serial number 60/288,200 filed May 2, 2001 entitled "ASSET MANAGEMENT SYSTEM" the contents of which are also incorporated herein by reference.

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The invention relates generally to the field of controlling, tracking, and managing access to assets or asset control devices by authorized users in a wide variety of sizes, locations, and types, including the ability to report and analyze the status and complete history of all inventoried assets at any time.

BACKGROUND ART

ASSETS

Assets by definition have intrinsic value and in some cases require security of some kind. Some assets are themselves secured but their security can be compromised through access to a control device such as a key, remote, badge, etc. in which case the control devices themselves require security.

One example of assets requiring security is the vehicle inventory of a car or truck dealership or fleet operator. In this example, the keys and remotes for each vehicle are the control devices to be secured such that (a) only authorized users have access to them (to prevent theft and vehicle damage liabilities) and (b) each authorized user is made accountable for the vehicle keys he/she removes from the secure environment.

Another example of assets requiring security is the door keys of apartment, condominium, office, school, medical, and other buildings or groups of buildings. In this example, the building or complex maintains no master keys but keeps the management key copies in a secured environment which controls access to authorized users and records the accountability of each authorized user of each key to reduce liabilities for personal harm, theft, damage, etc.

ASSET MANAGEMENT WITHOUT SECURITY

Typically, managers in the field of this invention have a hundred or hundreds of assets or asset control devices to be managed. This given, unsecured methods have evolved around organization of the assets such that they can be readily located for use.

In the car dealership example, a common method has been "pegboards" or an array of hooks mounted on a wall where each asset tag has an assigned hook which allows a particular asset to be located by its stock or other code number. Even in cases where the pegboard is mounted inside a locked cabinet, the cabinet is generally unlocked and open during business hours. This method presents a number of problems and liabilities for the dealer. One problem is that there is usually no indication what employee has taken an asset that is not currently on the board. Another problem is that only honesty and consistent application of dealership policies by all employees allows this method to work – typically, assets are not properly returned to their assigned hooks and may not be returned in a timely manner since employees understand that they have no accountability. An important liability is that employees, customers, or other visitors in the dealership have easy access to vehicle keys without detection or accountability in order to steal a vehicle or use it for unauthorized purposes – legal precedent clearly assigns liability to the dealership when it has poor security or lax procedures for security and its vehicles used by unauthorized drivers become involved in

personal or property damage accidents. Even in the absence of damage liability, vehicles may be damaged during their unauthorized use which causes repair costs to the dealer and possibly a lost sale if the damage is discovered in the process of conducting a prospect demonstration ride.

In the apartment or multi-family housing example, managers generally have a number of master keys which can unlock any apartment door and are assigned to specific managers, custodians, and maintenance contractors. Problems and liabilities arise because master keys can be (illegally) copied so there is no definitive way to know how many keys exist. Nor is there any accountability for each master key holder for his supervision of the key at all times and no way for management or the key holders to prove or disprove any use of the key in any apartment unit door by any master key holder. If management determines a breach of master key security, its only recourse is to re-key all apartment units and re-establish security but at a significant cost to management and with some irritation for tenants. More serious is the potential liability of tenants who may be injured during a break-in by a master key holder or who reports theft of possessions or damage to their apartment due to unauthorized entry, none of which can be aggressively disputed by management.

SECURED ASSET MANAGEMENT WITHOUT ACCOUNTABILITY

As a result of the serious liability potential and significant costs of unsecured asset management, there have been and are still sold today in the market of this field systems or methods which provide some level of security for the assets but no accountability for even authorized users.

One such system requires badge and/or password identification of authorized users in order to electronically open a secure enclosure of assets – however, once opened, the system relies on the honesty and policy compliance of the users to properly record all of the assets they remove. With no way to prove perfect compliance among all of its users, asset managers limit only their liabilities related to casual or negligent theft but still bear the burden of proof in all other cases.

Another specific method still in use involves a locked box attached to the asset, possibly a vehicle in a car dealership or the door of a vacant apartment. While providing some security against casual theft, lock boxes once opened by an authorized user or broken into by an unauthorized user provide no accountability for the use of the secured key. In addition, this method usually results in the keys in lock boxes being attached to the asset they protect after business hours and in the least secure environments for theft.

SECURED ASSET MANAGEMENT WITH ACCOUNTABILITY

There are also systems in which assets can be secured with accountability but no application of low-frequency RFID technology. In prior mechanisms, technologies which include but are no limited to bar codes and contact-based semiconductors have been used with grids where the location of tags with bar codes and/or chips are identified by x-y coordinates. These currently existing mechanisms are inadequate or undesirable because of their high cost, limited density, restricted enclosure specifications, and/or user inefficiencies in locating tags by coordinates.

Known prior art includes U.S. Patent 6,075,441 entitled "Inventoriable-Object Control and Tracking System, the disclosure of which is hereby incorporated by reference herein.

An object of this invention is to provide an improved asset management system that is more functional with more features than prior art systems.

Another object of this invention is to provide an improved asset management system that is more economical to manufacture with greater reliability than prior art systems.

These objects should be construed to be merely illustrative of some of the more prominent features and applications of the intended invention. Many other beneficial results can be obtained by applying the disclosed

invention in a different manner or by modifying the invention within the scope of the disclosure. Accordingly, other objects and a more comprehensive understanding of the invention may be obtained by referring to the summary of the invention, and the detailed description of the preferred embodiment in addition to the scope of the invention defined by the claims taken in conjunction with the accompanying drawings.

SUMMARY OF THE INVENTION

The invention is defined by the appended claims with the specific embodiment shown in the attached drawings. For the purposes of summarizing the invention, the invention comprises a computerized system for the tracking, and management of assets and/or asset control devices stored in one or more secure enclosures. The system manages authorizations for user access and administrative purposes and maintains complete histories and audit trails for the access of each asset or asset control device in the system.

The system allows for assets or asset control devices to be attached to tags containing passive low-frequency radio frequency transponders with unique identification numbers. The tags also function as light pipes in order for the system to indicate a specific tag to the user.

The secure enclosures of varying sizes and configurations each contain an array of RFID antennae and LED's mounted on or within "scanner" printed circuit boards. One or more "reader" printed circuit board assemblies

function to supply power, memory, and intelligent controls with which each position of the RFID arrays can be both scanned for the identification of a tag, if present, or flagged by lighting a LED which makes the tag visible to the user. For performance reasons, the reader maintains tables for the presence/absence of tags and for the full ID of present tags in all arrays. During the time a user has gained authorized access to the enclosure, the reader continuously scans all arrays and queues any access events in its memory. When the enclosure is secure and no user access is authorized, the reader performs periodic audit scans to assure the accuracy of its tables.

The system's controller computer software is alerted by any event in any security enclosure and subsequently responds to each event accordingly. The controller program function maintains a data base of the unique tag ID's with full descriptions of the assets they represent as well as complete histories of each tag access, including user, reason for access, date, and time. The controller also manages the functions of the enclosure, including opening, closing, locking, unlocking, status signals, warning and error conditions, etc.

The system's scalable software architecture allows not only multiple enclosures in each controller cluster but also multiple controller clusters in a local area network or multiple sites in an internet web-based network.

The foregoing has outlined rather broadly, the more pertinent and prominent features of the present invention. The detailed description of the invention that follows is offered so that the present contribution to the art

may be more fully appreciated. Additional features of the invention will be described hereinafter. These form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and the disclosed specific embodiment may be readily utilized as a basis for modifying or designing other methods and structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent structures do not depart from the spirit and scope of the invention as set forth in the appended claims.

BRIEF DESCRIPTION DRAWINGS

For a more succinct understanding of the nature and objects of the invention, reference should be directed to the following description taken in conjunction with the accompanying drawings in which:

FIG. 1 is an illustration of a transparent tag with a RFID chip.

FIG. 1A is an illustration of a drawer with RFID Tags.

FIG. 2 is an illustration of a typical tag.

FIG. 3 is a drawer for housing numerous tags.

FIG. 4 is a depiction of RFID tags within the drawer.

FIG. 5 is a depiction of a scanner.

FIG. 6 is a side view of a drawer showing tags.

FIG. 7 is a view of a back panel of the housing.

FIG. 8 is a view of a key tag formed from an opaque plastic that serves as a light pipe for LED in the scanner board. An RFID transponder is inserted into a drilled out hole within the tag, which is thereafter sealed with an epoxy.

FIG. 9 is a view of a vacuum molded part for use within the drawer.

FIG. 10 is an internal view of the drawer.

FIG. 11 is an internal view of the drawer.

FIG. 12 is a side elevational view of several keys.

FIG. 13 is a schematic of the scanner of the present invention.

FIG. 14 is a schematic of the scanner of the present invention.

FIG. 15 is a schematic of the controller board of the present invention.

FIG. 16 is a flow chart of application software.

FIG. 17 is a flow chart of application software.

FIG. 18 is a flow chart of application software.

FIG. 19 is a flow chart of application software.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Components Of The System

The invented system and its components utilize RFID (Radio Frequency Identification) technology to store and locate assets or asset control devices within security enclosures of a wide range of sizes and configurations. The common elements of the invention include:

Tags

Opaque plastic rods or hooks of various sizes and shapes which contain embedded passive low-frequency RFID transponders with unique identification codes and also serve as light pipes. The assets or asset control devices are securely attached to the tags. Tags may be re-used in cases where the assets associated with them have been retired or replaced. Tags are designed such that they can be placed in arrays within security enclosures such that RFID transceivers can activate and read the unique tag ID's and subsequently identify the associated asset. Figures 1 and 2 illustrate the tags that can be employed with the present invention.

Security Enclosures

A wide variety of horizontal, drawer-mounted or vertical, wall- or cabinet-mounted racks which allow tags and their attached assets or asset control devices to be inserted, stored, and removed. The system controls the functions of the security enclosure such that only authorized users can gain

access. Further, once accessed the system assigns accountability for each tag removed to the authorized user, recording the date, time, and reason for use. Each enclosure must have capabilities to be opened and closed and/or locked and unlocked electronically and for its security status to be determined electronically by the system. Figures 3-11 are photographs of a security enclosure comprising a drawer.

Scanner Boards

An array of RFID transceivers and LED's where densely stored tags can be reliably read without collision of radio frequencies and individual tags can be caused to flash red and easily located in the array by users. Each security enclosure is populated with one or more scanner boards, all of which are connected to reader boards. Figures 13-19 include schematics, firmware and application software, and operational flow of the scanner boards.

Reader Boards

Each reader board controls one or more scanner boards and causes the array of transceivers to be scanned continuously. The reader maintains a table of array locations where tags are present and absent and a table of unique tag ID's for all locations where tags are present. During its continuous scan, any change in tags is an event recorded in an event queue which causes notification to the system's controller software. The reader can also cause the LED at a specific array location to be lit on direction of the system controller software which identifies the tag being requested by a user.

The reader also performs a full audit scan of all tag ID's present on closure of the security enclosure and periodically thereafter until the enclosure is re-opened and continuous scanning is re-started. Figures 13-19 include schematics, firmware and application software, and operational flow of the scanner boards.

External Tag Reader

Each enclosure, cluster of enclosures, or group of enclosure clusters must include at least one external tag reader which may be electronically attached to the reader board, controller computer, or host computer. The external tag reader is used administratively to assign unique tags to their associated assets or asset control devices and may also be used to identify authorized users. The form of the external tag reader is such that its placement and use for its intended purposes is suitable. See photographs Figures 3-11.

User Identification Device

Users are identified to the system by typing a user name, applying a RFID badge or tag, or through the use of some other identification means, including biometric devices such as thumbprint, fingerprint, or retinal scanners. The external tag reader may be used for this purpose where uniquely assigned RFID tags or badges are issued to authorized users (see Figures 3-11). Optionally, the system may also require entry of a user-specific password. A user identification device must be located in the vicinity

of the security enclosure(s) it serves; the system will not allow "remote" access to a security enclosure.

Software

The system software contains a number of elements which can be operated in a wide variety of configurations. The scalability of the architecture allows many physically varied installations as well as the management of the system in different ways. Scanner and reader software programs reside on the scanner and reader boards respectively and perform the functions described above. Controller software programs may manage multiple readers or groups of readers in different physical locations and the input and display devices of the user interface at the location of the security enclosures. Host application software maintains a data base of all assets and their associated unique ID's, the complete history of their use, the complete history of user access, displaying and printing reports and analyses of asset usage, etc. Figures 13-19 include schematics, firmware and application software, and operational flow of the scanner boards.

RFID Primer Notes

Of the variations of radio frequency identification technologies, the system specifically uses passive low-frequency technology. The transponders have no battery or other power source but are "wakened" by a transceiver issuing a signal that contains sufficient power for the transponder's response of its unique ID.

Since communication is radio frequency, the system does not require contact between the transceiver and transponder to function. The distance between them is a function of the signal strength, environmental conditions, and other factors. Control of the distance is also important to minimize collision, where a single transceiver may activate and obtain responses from multiple transponders – these situations can sometimes be managed through sophisticated software. This invention eliminates collision by its careful design of the RF communications parameters. See the drawing of Figures 3-11 showing the relative positioning of the keys containing the transponders above the receivers that minimizes collisions.

The transponders are protected by embedding them in the plastic tags and sealing them with epoxy. They are then waterproof, relatively heat and cold resistant, and safely attached to the asset/device where the tag itself is strong and durable.

SOFTWARE FUNCTIONS

Notes On Software

- Since the software is Windows-based, navigation on user interface screens may be done with a mouse, but may also be done with only keyboard strokes. Most installations are expected to avoid using a mouse.
- Most fields are associated with pre-defined lists of responses and "auto fill" as users begin to type characters – when the selected response is

displayed and highlighted in the field, the user may select it without additional typing by moving to the next entry field. Fields also have drop-down lists of the choices which may be accessed and selected with a mouse, if available.

Assigning Tags To Assets

A function of the host software program allows an authorized administrative user to add an asset to the system by importing or entering the description of the asset and associating the asset with a unique tag by "touching" the tag to an external tag reader and physically attaching the asset or asset control device to the tag. The asset is accountable to the administrative user until it is returned to a security enclosure.

Removing An Asset Tag

The system displays a default "log-in" screen – no system function may be initiated by a user without first being confirmed as an authorized user. The user presents a badge or fingerprint if such user identification option is attached to the system or types his user name and, optionally, his password. The system displays a message if the user ID or name and password do not match in the system's authorization table which allows specified classes of users to perform specified functions. The authorized user may repeat his attempt to log in. The system records all rejected log-in attempts for possible future analysis of security breaches.

The user removing a key selects from 2 options:

QuickKey – the user enters one or more asset numbers (such as vehicle stock numbers) directly on the log-in screen. The system displays the "check out reason" screen containing a pre-defined list of reasons for removing keys. The user selects a reason for each asset requested. The system displays all assets currently assigned to the user's accountability, opens the enclosure, displays the "enclosure open" screen, and lights one of the selected asset tags. On removal of the lighted tag, the system lights the next selected tag, if any. The user may at any time remove other asset tags which have not been requested. Each asset removed, whether or not requested on the log-in screen, is added to the user's accountability display. The system displays messages for cases in which an asset is currently checked out to another user or the asset ID is invalid. For each asset tag removed, the user's accountability display includes the asset ID, asset description, and reason and/or location. While the enclosure is open, the user may return asset tags which have been removed in prior or the current access period – the display requests the location of assets returned per below.

FindKey – users who do not know the asset ID's to be removed may use the system's search engine by leaving the asset ID field on the log-in screen blank. The "search" screen is displayed which allows

the user to select one or more pre-defined asset description fields. The system performs "and" logic operations when the user selects multiple description fields to search and "or" logic operations for any multiple choices for each description field. As the user refines search parameters, the display updates a summary view of the search parameters and the number of matching assets. On completing the search definition entry, the system displays the "check out reason" screen for each asset selected and subsequently displays the "drawer open" screen, opens the drawer, and lights one of the selected asset tags. An example of a search for a car dealership would be to find all "new Mustang convertibles" (using 3 predefined description fields of new/used, model, and body type) – if there are 5 matching vehicles in inventory, the appropriate key tags will be lighted.

Returning An Asset Tag

The user may choose to return an asset tag on the log-in screen. The system displays the enclosure open screen and opens the enclosure. As each asset tag is returned to any open position in the available arrays, the system displays the "location" screen from which the user selects a response indicating the location of the asset at the time of the tag return. While the enclosure is open, the user may remove other asset tags (which prompts the reason screen and adds the asset to his list) or may initiate either of the

QuickKey or FindKey functions. The system displays a message if any tag is returned which is not currently assigned to an asset in the system.

Retiring An Asset

A function of the host software program allows properly authorized administrative users to "delete" assets from the system. While retiring the asset functions as a deletion so far as the asset tag is concerned (the asset tag may then be re-assigned to another asset), the system archives the history of the retired asset for further use and analysis.

Administrative Functions

In addition to adding and retiring assets, authorized administrative users may add and delete users along with assigning their badge or tag ID's, authorization classes, and passwords. Administrative users may display or print standard reports defined in the system or use the adjunct report generation function to create reports. Administrative users maintain the pre-defined lists used in the system for user selection in auto-fill and drop-down menus.

System Administration Functions

One or more authorized system administrators may alter the system configuration, change the field definitions used for pre-defined lists, and modify other system functions to account for changes over time in the system environment.

CURRENT HARDWARE IMPLEMENTATION

The current hardware implementation is targeted at vehicle dealerships, vehicle fleet operators, and multi-family housing managers. The assets to be managed are vehicle keys and remotes or apartment keys. The enclosure is a security drawer made from 16-gauge steel with an array of 256 key tag locations.

DRAWERS

Other drawer configurations are in development, including a "mini" drawer with approximately 150 tags and a "combo" drawer that is used to control license plates as well as keys.

In the longer term, an enclosure may be a locked room and arrays of scanner boards can be mounted on walls or in filing cabinets, etc. to control assets such as expensive electronic devices or documents/files. An example of other enclosure designs is a current opportunity to control hand- or wrist-mounted bar code scanners worn by employees of package delivery firms.

TAGS

Tags are currently 6.5" long plastic rods into which a transponder is inserted in one end and sealed with epoxy. The top end is drilled for a key ring or rivet with which to attach the keys and remotes, generally along with a printed tag or card with asset description information. The "production" version of the tags currently in design uses a "hook" shape so keys hang down when attached and a détente on the transponder end to provide a "click" feel

when the tag is properly inserted. Two unique and critical properties of the tags are:

RFID – there is no known use of RFID technology in the field. One of the tag advantages of RFID is its non-contact read capability which allows opportunities to protect the drawer electronics with a mylar sheet and elimination of wear and tear failures of contact type tags.

Light pipe – the tags also function as light pipes which allows the system to indicate selected tags to the user without using an x-y grid position for which the user must search on a silk-screened drawer insert.

SCANNER BOARDS

In the current drawer, 4 scanner boards with an 8x8 array of transceivers are connected to 4 plastic inserts and a drawer-size metal cover. Cables are attached to a connector. The scanner board assembly is inserted into the drawer and a cable is attached from the connector to the reader board attached to the back of the drawer cabinet. The "production" scanner boards will be surface mount assemblies with a "bobbin" assembly for each transceiver/LED. Each scanner board contains a processor (EEPROM) and small Assembly program with other electronics.

NOTE: A unique and critical property of the RFID design is that a large number of transponders in a very small space can be reliably read without collision. Even engineers familiar with RFID would say this can't be done – the "normal" implementation would be to create a

"field" through which transponders would pass and be read – this is used in many active higher-frequency RFID applications (toll roads) and in some passive applications under development (grocery store checkout). An alternative "normal" implementation would be to create a single "read field" in the drawer whereby one transceiver would communicate with all of the tags – this requires collision detection that is probably beyond the capabilities of current software and presents other problems associated with the size of the field (for example, the scanner may read tags which are located outside the closed drawer) – the use of metal in the drawer and the presence of metal in the keys and remotes also present technical scanning issues for defining the reading environment.

READER BOARDS

The reader board assembly manages power (from an external "brick" power source), drawer functions such as open, close (de-energize solenoid), lock, and unlock. The reader board also controls an external status LED that can be lighted green, red, or both to indicate status such as power on. The reader board includes a processor (EEPROM) and memory for the presence/absence table, tag ID table, and event queue.

DRAWER INTERFACE

The drawers use a modified parallel interface to a PC which functions as the drawer or drawer cluster controller. The parallel protocol is modified

to include drawer ID so that up to 8 drawers may be daisy-chained to a single parallel PC port. The reader board programs ignore any command which does not include its drawer ID.

SCALABILITY

The system is designed to be very flexible in its configuration and operation. While the function and location of the scanner and reader board "firmware" is not affected, other software components will operate differently.

Multiple Drawers

While an entire system may be a single drawer and a single PC, up to 8 drawers may be connected on the parallel port. In these single-cluster systems, the controller and host software will run on the PC and a printer, an external reader, and optional user identification device will be attached. The software functions described above are somewhat complicated by the need to open the drawer(s) which contain the requested tags – they must be opened one at a time. Tags can be returned to any drawer in the cluster, normally according to which has the most unused positions.

Multiple Clusters/Network Configuration

In larger car dealerships, for example, clusters of one or more drawers each will be installed in different locations – new car, used car, get ready department, service department, etc. In these cases, each cluster will be controlled by a PC (or integrated controller) which in turn is connected to a new or existing LAN. One PC on the LAN will then serve as the host and

coordinate activity of the clusters. All LAN users who are authorized may access the host software for reports, etc. at their LAN workstations. LAN's with remote access capability could also allow remote access to host software functions. One or more external tag readers can be attached to any LAN workstations for administrative users to add assets and employees. User identification must always be performed at the cluster location.

Integrated Controller

An early hardware development will be to eliminate the current cluster PC in favor of an integrated, dedicated PC containing only the specific capabilities required by the system controller functions. The mouse, keyboard, and CRT will be replaced by a touch screen. With integrated controllers, a separate LAN-connected host PC is required.

Web Configuration

In a future development, the host software functions will be executed from the web. In multi-site environments (for example, car dealers with multiple stores), the system would have all asset information available and could perform additional functions related to summarizing activity at all sites. We may also "license" the system usage as monitored on the web instead of "selling" software and/or hardware.

SYSTEM DESCRIPTION
KEYSMART ASSET MANAGEMENT SYSTEM

1. Overview

The KeySmart Asset Management System is a product that allows the consumer to monitor assets moving into and out of central location. The function of the System is to 1) hold any user of the asset accountable while he has the asset checked out; and, 2) decrease the time it takes to locate an asset. The assets of choice for initial product rollout are keys. These assets will be secured in a drawer; and any activities concerning the keys will be controlled via computer software.

The primary target markets for KeySmart are auto dealerships, apartments, office buildings, schools, vehicle fleet owners (rental car agencies, trucking companies, etc.), valet service, etc.

2. Definitions

- Cluster: Node containing PC, UPS (as needed) and one or more drawers.

- System: Complete package including Cluster, Master Control Software, and any other software module.

- Drawer: Consists of enclosure that houses the drawer and the drawer.

- RFID components

    - An antenna or coil. An antenna is used to transmit information from a reader to a tag, and to receive information sent by a tag. The size and format of an antenna will reflect the specific application, and may range from a small circular coil to large planar structures suitable for access control systems.
    - A transceiver (with decoder). A "reader" is an electronic unit that transfers information to and from one or more tags (it should be noted that the term reader is used interchangeably to mean both a read only and read/write unit). The size and features of a reader may vary considerably, and it may operate in isolation, or be connected to a remote computer system.
    - A transponder (commonly called an RF tag) that is electronically programmed with unique information. A tag is a small electronic circuit, usually encased in glass or plastic, which in its simplest form contains a unique identification code that may be "read", without contact or line of

sight, by suitable electronics. More sophisticated tags may also store information generated by the user, again without contact or line of sight.

3. Product Evolution Plan

Version 1.0	One cluster containing one drawer
Version 1.1	One cluster containing multiple drawers
Version 1.2	Multiple clusters connected on a network
Version 1.3	System is web enabled
Version 2.0	Embed PC functions
Future	Higher security features (biometrics, video surveillance); Ability to locate tag on premise; Increase the density/amount of tags per drawer;

4. System Requirements

- Should be able to easily handle different types/sizes of assets
- Building block type technology to go from 50 assets up to 2500 assets
- Building block technology must allow different entry levels of security

5. Main Components

5.1 *Cluster Controller – Personal Computer*

Requirements:

- Monitor
- Keyboard
- Keypad
- (?) MHz Processor
- (?) Memory
- RAM
- (?) Disk Space

5.2 Peripherals

5.2.1 Single RFID Antenna/Reader

Interface: Connection via USB or RS-232C

Certification: FCC Class B/UL/CSA

The single RFID antenna/reader may be used to 1) identify the individual who is requesting access to the system; or 2) assign new assets to tags; or 3) allow customer the ability to perform administrative functions on a remote PC.

5.2.2 Drawer(s)

Interface: Connected via USB.

Certification: FCC Class B/UL/CSA

Contents: Three sizes depending on the number of tags: 50, 100, or 300 tags.

Requirements:

- Status LEDs on drawer
- Spring loaded?
- Provides mounting points for RFID equipment in drawer
- Manual release
- Physical size. ~ 19" to 23" wide x 10" high x ~ 27" to 30" deep
- Stackable
- Power requirements: to be determined. Either external power brick or internal power supply
- Drawer ID to differentiate between multiple drawers

Figure 1 shows a typical drawer.

5.2.2.1 Physical Characteristics

The enclosure will house the assets in drawer(s). It will be made of 16 or 18 gauge steel and contain one or more drawers. The drawers will be capable of full extension, riding on steel ball-bearing drawer slides, to allow access to entire contents of drawer. The construction of the enclosure should "discourage" unauthorized entry but need not be "burglar-proof" – i.e. it's not a safe but it should not be violated without damage.

There will be two methods of opening the drawer 1) manual release with a key (in case of power outage); and 2) electronic via solenoid. Under power, the System will ensure that only one drawer can be opened at a time. Access between drawers will be discouraged.

*5.2.2.2. **Plastic Insert***

Function/Requirement:

- hold the tags in position – right side up;
- provide detent for user feed back to ensure tag fully seated
- keep tags, not properly inserted into the receptacle, away from the RFID antenna
- fix the read distance of the tag to the antenna
- as needed, provide a foundation for attaching labels/demarcations within the drawer
- able to hold the weight of the assets (max. 30 lbs.)
- contains integral receptacles to accept RFID tags
- should keep liquids and/or debris from falling to the bottom of the drawer

The plastic insert sits on the bottom of the drawer above the RFID antenna.

*5.2.2.3 **Release***

Function/Requirement:

- Solenoid for latch to open the drawer. Includes a state switch to determine if the drawer is "open" or "closed".

*5.2.2.4 **Tag***

Function/Requirement

- Includes the RFID tag
- Each RFID tag should have a unique ID
- Diagnostic functions (?)
- Environmentally sealed
- Hook or eyelet for attaching assets (keys)
- Rugged

- Low cost

Figure 2 shows a typical tag.

The tag will consist of a simple RFID chip that will be energized by the magnetic field created by the antenna closest to it. Installed on the circuit board are the LED's and the antennas. Each hole has an LED to indicate to the user that the transponder inserted in that slot is being enabled. If the controller stops the polling process at any individual transponder, that LED will remain lit. The LED is located dead center in the hole and beamed upward to cause the transponder to act as a light pipe. When the transponder is "flagged" the LED causes the transponder to glow and be easily identified for the user to pull out.

5.2.2.5 Reader/Antennae

Function/Requirement:

- Controlled read range should be < 2cm
- FCC Class B
- Read time for fully loaded drawer (300 tags) should be less than or equal to 2 seconds
- Detect rogue tags
- Power
- Continuous reading capability
- Interface to USB micro controller

Program mode, ability to add a new tag/asset to the system within existing system in a timely manner.

A printed circuit board (PCB), containing antennae and LED's (light emitting diode) will be located on the inside bottom surface of the drawer. There will be one antenna and one LED per asset slot. The LED will blink on command and act as a visual asset locator for the user. The RF antenna system will consist of approximately 96 individual antennas arranged in an X-Y matrix. Each antenna will be polled by the reader electronics and if a transponder is present, it will be read and the data sent to a PC or other controller for inclusion into a database.

The antenna system will be made up of smaller antenna boards of 8 x 12 antenna's. These boards can be stacked in various arrangements to make up different size drawers. Details will be worked out at a later date.

The RFID implementation must distinguish between tags in a drawer from tags in other, stacked drawers and/or tags near or on top of drawers and security enclosures. In

addition, tags should be properly placed into plastic insert receptacles in order to be read. For these reasons, the read range is limited to < 2cm above the antenna PCB.

Each drawer should be the highest tag capacity practical for (a) the interrogator to accurately, reliably, and quickly identify all tags and (b) the grid design to organize tags.

5.2.2.6 Drawer Device Drive Module

Software to provide an application programming interface to hardware.

Functions:

- Open drawer
- Drawer state
- Scanning tags (full count)
- Tag Diagnostic (light all tags to ensure tag function)
- Tell the LEDs beneath the requested tag(s) to blink

5.2.3 Uninterruptable Power Supply

An optional uninterruptable power supply can be provided in order to provide power to the System during power outages.

6. Proposed Method of Operation

6.1 *System Operation (find key)*

Assume: Drawer is loaded with tags (anywhere from 0 to 300 tags at any given time). User is at an enclosure that contains the asset.

- User inserts his ID "key" and enters his PIN.
- He queries the asset monitoring system for the location of the key.
- The monitoring system identifies drawer and activates RFID reader/antennae (locator) in drawer to verify asset.
- The reader sends a signal to the RFID tag and starts the LED blinking.
- The monitoring system unlocks the drawer.
- The user visually locates the tag and removes it from the drawer.

- The reader informs monitoring system of requested tag(s) removal (and any other tag that is missing) in real time.
- The user closes the drawer.
- The monitoring system verifies drawer closure and deactivates the electronics in the drawer.
- The monitoring system logs the transaction, charges user for asset(s) checked out.

6.2 *System Operation (replace key)*

Assume: User is at an enclosure that can hold the asset.

- User inserts his ID "key" and enters his PIN.
- He queries asset monitoring system for drawer space to return key.
- System identifies a drawer, activates the RFID reader, and unlocks it.
- User inserts tag into an empty receptacle.
- The reader informs monitoring system of tag(s) return in real time.
- The user closes the drawer.
- The monitoring system verifies drawer closure and deactivates the electronics in the drawer.
- The monitoring system logs the transaction, records return of asset(s).

The present invention includes that contained in the appended claim as well as that of the foregoing description. Although this description has been described in its preferred form with a certain degree of particularity, it should be understood that the present disclosure of the preferred form has been made only by way of example and that numerous changes in the details of construction, combination, or arrangement of parts thereof may be resorted to without departing from the spirit and scope of the invention.

Now that the invention has been described,